(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 44 13 678 C 1**

(51) Int. Cl.[6]:
H 04 N 1/44
H 04 N 1/32
H 04 L 9/32

(21) Aktenzeichen: P 44 13 678.1-31
(22) Anmeldetag: 20. 4. 94
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 4. 5. 95

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Müller, Horst, 36251 Bad Hersfeld, DE; Römmeling, Gerhard, 36251 Ludwigsau, DE

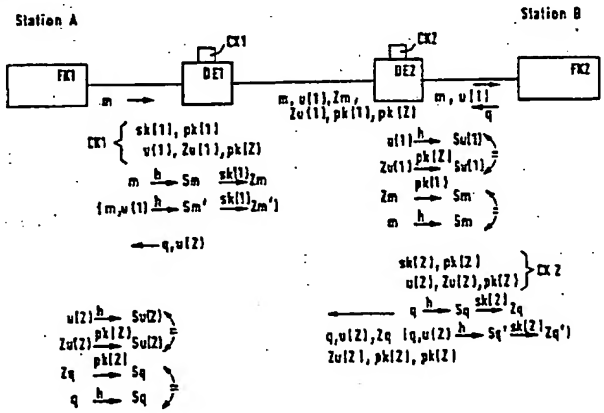
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE	33 03 846 A1
US	50 05 200
EP	5 47 837 A2
EP	3 84 475 A1

DE-B.: BITZER, Wolfgang: Verschlüsselte Textübertragung. In: NTG-Fachberichte, Bd.74, Text- und Bildkommunikation, VDE- Verlag GmbH, Berlin, 1980, S.109-117;

(54) Elektronisches Einschreibeverfahren bei der Datenübertragung

(57) Die Erfindung betrifft ein elektronisches Einschreibeverfahren, bei dem ein zu übertragender Datensatz (m) eines Dokumentes signiert und zertifiziert wird, ein Datensatz (u(1)) einer persönlichen Unterschrift ist gesichert mit einem Unterschriften-Zertifikat (Zu(1)) abgespeichert, die Datensätze (m, u(1)), die beiden Zertifikate (Zm, Zu(1)) sowie die dazugehörigen Schlüssel (pk(1), pk(Z)) werden zu einer Empfangsstation übertragen, dort werden die Datensätze (m, u(1)) mit den Zertifikaten (Zm, Zu(1)) auf Unversehrtheit überprüft, ein zurückzuübertragender Datensatz (q) einer Quittung wird signiert und zertifiziert und analog wie der Dokumenten-Datensatz mit einem weiteren gesicherten Unterschriften-Datensatz (u(2)) übertragen und überprüft.



Beschreibung

Die Erfindung betrifft ein Einschreibeverfahren für ein elektronisch übertragenes Dokument.

Durch Verwendung von Fernkopierern können Dokumente auf elektronischem Wege übertragen werden. Solche Dokumente werden aber nicht rechtsverbindlich anerkannt, da sendeseitige Manipulationen nicht ausgeschlossen werden können. Solche Manipulationen sind beispielsweise das Hineinkopieren der Unterschrift einer Person, die das Dokument nie gesehen hat.

Es ist ein elektronisches Einschreiben bekannt (DE-B.: Bitzer, Wolfgang: Verschlüsselte Textübertragung. In: NTG-Fachberichte, Bd. 74, Text- und Bildkommunikation; UDE-Verlag GmbH, Berlin, 1980, Seite 109 bis 117), bei dem der zu übertragende Text über eine Schlüsselverteilzentrale zu einem Empfänger übertragen wird. In der Schlüsselverteilzentrale wird der Text mit einer elektronischen Unterschrift signiert. Als Empfangsbeweis kann als Quittung die Signatur über die Schlüsselverteilzentrale zum Absender zurückgeschickt werden.

Aus der EP 05 47 837 A2 ist ein System zur Authentifizierung bekannt, bei dem auf dem zu übertragenden Textbogen eine Signatur aufgebracht wird.

Der Erfindung liegt die Aufgabe zugrunde ein elektronisches Einschreibeverfahren für ein solches Dokument anzugeben, bei dem die Unterschriften für das Dokument und die Quittung fälschungssicher übertragen werden.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

Im folgenden wird die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispieles beschrieben.

In der einzigen Figur sind als Blockschaltbild einige Hardwarekomponenten dargestellt, anhand derer die Durchführung des erfindungsgemäßen Verfahrens erläutert wird. Es wird davon ausgegangen, daß ein Dokument von einer Station A zu einer Station B übertragen wird. Hierzu weist die Station A einen Fernkopierer FK1 und die Station B einen Fernkopierer FK2 auf. In der Station A ist weiter eine Datensicherungseinrichtung DE1 und in der Station B eine Datensicherungseinrichtung DE2 vorgesehen. Mit der Datensicherungseinrichtung DE1 ist eine Chipkarte CK1 kontaktiert, so daß ein wechselseitiger Datenaustausch zwischen der Datensicherungseinrichtung DE1 und der Chipkarte CK1 durchgeführt werden kann. Analog ist auch auf der Empfangsseite eine Chipkarte CK2 mit der Datensicherungseinrichtung DE2 kontaktiert.

In der sendeseitigen Station A wird im Fernkopierer FK1 aus einem nicht dargestellten Dokument ein Dokumenten-Datensatz m gebildet. Dieser Datensatz m wird zur Datensicherungseinrichtung DE1 übertragen und dort vor der Aussendung zur Station B bearbeitet.

Der Urheber des zum Datensatz m gehörenden Dokumentes hat die Chipkarte CK1 mit der Datensicherungseinrichtung DE1 kontaktiert. Diese Chipkarte CK1 ist beispielsweise eine Cryptochipkarte, und der Urheber hat sich durch ein an sich bekanntes Sicherungsverfahren, wie beispielsweise eine PIN (persönliche Identifikationsnummer), ein Paßwort oder ein biometrische Verfahren gegenüber der Chipkarte CK1 und der Datensicherungseinrichtung DE1 identifiziert.

Der Dokumenten-Datensatz m wird in der Datensicherungseinrichtung DE1 selbst oder in der Chipkarte CK1 signiert, d. h. aus dem Datensatz m wird beispielsweise durch ein Hashverfahren h eine Signatur Sm gewonnen. Zur Durchführung dieser Operation auf der Chipkarte CK1 muß diese eine entsprechende Rechnerkapazität aufweisen.

Auf der Chipkarte CK1 sind beispielsweise ein geheimer und ein öffentlicher Schlüssel sk(1), pk(1) des Urhebers gespeichert. Diese beiden Schlüssel sk(1), pk(1) (secrete key, public key) und ihre Eigenschaften sind als Bestandteile des sogenannten Public-Key-Verfahrens bekannt.

Weiter ist auf der Chipkarte CK1 die Unterschrift des Urhebers abgespeichert. Diese Unterschrift wurde beispielsweise durch Abtastung der Originalunterschrift des Urhebers gewonnen und in digitalisierter Form als Datensatz u(1) abgespeichert. Auf der Chipkarte CK1 ist ein öffentlicher Schlüssel pk(Z) abgespeichert. Dieser Schlüssel pk(Z) gehört zu einem geheimen Schlüssel sk(Z), mit dem beispielsweise in einer Zertifizierungsstelle die persönliche Unterschrift gesichert auf der Chipkarte CK1 abgespeichert wurde. Zur Sicherung wurde in der Zertifizierungsstelle aus dem Unterschriften-Datensatz u(1) mit einem Hashverfahren h eine Signatur Su(1) errechnet. Mit dem geheimen Schlüssel sk(Z) der Zertifizierungsstelle wurde aus der Unterschriften-Signatur Su(1) durch ein asymmetrisches Kryptierverfahren ein Zertifikat Zu(1) gebildet. Dieses Zertifikat Zu(1) ist ebenfalls auf der Chipkarte CK1 abgespeichert.

Aus der Signatur Sm des Dokumenten-Datensatzes m wird mit Hilfe des Geheimschlüssels sk(1) des Urhebers durch das asymmetrisches Kryptierverfahren ein Zertifikat Zm gewonnen.

Von der Datensicherungseinrichtung DE1 der Station A werden folgende Daten an die Datensicherungseinrichtung DE2 der Station B gesendet: Der Dokumenten-Datensatz m, der Unterschriften-Datensatz u(1), das Zertifikat Zm und das Zertifikat Zu(1), sowie die zu den geheimen Schlüsseln sk(1) und sk(Z) gehörenden öffentlichen Schlüssel pk(1) und pk(Z) des Urhebers und der Zertifizierungsstelle.

Bei der Verwendung des asymetrischen Kryptierverfahrens ist der öffentliche Schlüssel pk(1) der zu dem Zertifikat Zm, und der öffentliche Schlüssel pk(Z) der zu dem Zertifikat Zu(1) gehörige Schlüssel, da nur mit ihnen aus den Zertifikaten Zm, Zu(1) die entsprechenden Signaturen Sm, Su(1) zurückgewonnen werden können.

Innerhalb der Datensicherungseinrichtung DE2 oder/und auf der Chipkarte CK2 der Station B werden die folgenden Überprüfungen vorgenommen.

In einem ersten Schritt wird der empfangene Unterschriften-Datensatz u(1) mit dem Zertifikat Zu(1) auf Unversehrtheit geprüft. Hierzu wird aus dem Datensatz u(1) über das Hashverfahren h empfangsseitig die Signatur Su(1) gewonnen. Auf einem zweiten Weg wird diese Signatur Su(1) über den öffentlichen Schlüssel pk(Z) aus dem Zertifikat Zu(1) gewonnen. Bei Gleichheit dieser beiden gewonnenen Signaturen Su(1) kann auf die Unversehrtheit der Unterschrift bzw. des zugehörigen Datensatzes u(1) geschlossen werden.

In einem zweiten Schritt wird der empfangene Dokumenten-Datensatz m mit dem Zertifikat Zm auf Unversehrtheit geprüft. Hierzu wird mit dem Hashverfahren h aus dem Datensatz m die Signatur Sm berechnet. Auf einem zweiten Weg wird diese Signatur Sm über den öffentlichen Schlüssel pk(1) aus dem Zertifikat Zm gebildet. Bei Gleichheit dieser beiden Signaturen Sm kann auf die Unversehrtheit des Dokumentes bzw. des zugehörigen Datensatzes m geschlossen werden.

Von der Datensicherungseinrichtung DE2 werden dann die Datensätze m, u(1) des Dokumentes und der Unterschrift an den Fernkopierer Fk2 gegeben. Auf dem Fernkopierer Fk2 kann dann das aus dem Datensatz m reproduzierte Dokument zusammen mit der aus dem Datensatz u(1) reproduzierten Unterschrift ausgedruckt werden. Auch eine schriftliche Darstellung auf einem Bildschirm ist möglich.

Durch das erfindungsgemäße Verfahren ist sichergestellt, daß das empfangsseitig dargestellte, mit einer Unterschrift versehene Dokument mit der Unterschrift des tatsächlichen Urhebers unterzeichnet ist.

Bei einer Variante zu diesem Verfahrensabschnitt wird in der sendenden Station A eine Signatur Sm' aus dem Dokumenten- zusammen mit dem Unterschriften-Datensatz m, u(1) gebildet. Aus dieser Signatur Sm' wird mit dem geheimen Schlüssel sk(1) des Urhebers ein Zertifikat Zm' errechnet. In der empfangenden Station B wird dann die Prüfung mit diesen Werten durchgeführt.

Zur Realisierung des Einschreibeverfahrens wird von der Station B automatisch nach dem Empfang des unterzeichneten Dokumentes und seiner Überprüfung eine von einem Empfänger unterschriebene Quittung an die Station A zurückübertragen.

Hierzu wird beispielsweise im Fernkopierer FK2 der Station B aus einer nicht dargestellten Quittung ein Datensatz q gebildet. Dieser Quittungs-Datensatz q wird zur Datensicherungseinrichtung DE2 übertragen und dort vor der Aussendung zu Station A bearbeitet.

Der Empfänger, der das Dokument von der Station A erhalten hat und die Quittung unterzeichnet, hat sich analog, wie der Urheber in der Station A, gegenüber der Chipkarte CK2 und der Datensicherungseinrichtung DE2 in der Station B identifiziert.

Der Quittungs-Datensatz q wird in der Datensicherungseinrichtung DE2 selbst oder in der Chipkarte CK2 signiert, d. h. aus dem Datensatz q wird durch das Hashverfahren h eine Signatur Sq gewonnen. Zur Durchführung dieser Operation auf der Chipkarte CK2 muß diese eine entsprechende Rechnerkapazität aufweisen.

Auf der Chipkarte CK2 sind ein geheimer und ein öffentlicher Schlüssel sk(2), pk(2) des Empfängers gespeichert. Weiter ist auf der Chipkarte CK2 die Unterschrift des Empfängers abgespeichert. Diese Unterschrift wurde analog wie die des Urhebers gewonnen und in digitalisierter Form als Datensatz u(2) abgespeichert. Auf der Chipkarte CK2 ist auch der öffentliche Schlüssel pk(Z) der Zertifizierungsstelle (es kann sich hierbei um die gleiche vertrauenswürdige Instanz handeln die die Unterschrift des Urhebers auf der Chipkarte CK1 sicherte) abgespeichert, von der die persönliche Unterschrift des Empfängers gesichert auf der Chipkarte CK2 abgespeichert wurde. Zur Sicherung wurde in der Zertifizierungsstelle aus dem Unterschriften-Datensatz u(2) mit einem Hashverfahren h eine Signatur Su(2) errechnet. Mit dem geheimen Schlüssel sk(Z) der Zertifizierungsstelle wurde aus der Unterschriften-Signatur Su(2) durch ein asymmetrisches Kryptierverfahren ein Zertifikat Zu(2) gebildet. Dieses Zertifikat Zu(2) ist ebenfalls auf der Chipkarte CK2 abgespeichert.

Aus der Signatur Sq des Quittungs-Datensatzes q wird mit Hilfe des Geheimschlüssels sk(2) des Empfängers durch das asymmetrisches Kryptierverfahren ein Zertifikat Zq gewonnen.

Von der Datensicherungseinrichtung DE2 der Station B werden folgende Daten an die Datensicherungseinrichtung DE1 der Station A gesendet: Der Quittungs-Datensatz q, der Unterschriften-Datensatz u(2), das Zertifikat Zq und das Zertifikat Zu(2), sowie die zu den geheimen Schlüsseln sk(2) und sk(Z) gehörenden öffentlichen Schlüssel pk(2) und pk(Z) des Empfängers und der Zertifizierungsstelle.

Bei der Verwendung des asymetrischen Kryptierverfahrens ist der öffentliche Schlüssel pk(2) der zu dem Zertifikat Zq gehörige Schlüssel, da nur mit ihm aus dem Zertifikat Zq die entsprechende Signatur Sq zurückgewonnen werden kann.

Innerhalb der Datensicherungseinrichtung DE1 oder/und auf der Chipkarte CK1 der Station A werden die folgenden Überprüfungen vorgenommen.

In einem ersten Schritt wird der empfangene Unterschriften-Datensatz u(2) mit dem Zertifikat Zu(2) auf Unversehrtheit geprüft. Hierzu wird aus dem Datensatz u(2) über das Hashverfahren h empfangsseitig die Signatur Su(2) gewonnen. Auf einem zweiten Weg wird diese Signatur Su(2) über den öffentlichen Schlüssel pk(Z) aus dem Zertifikat Zu(2) gewonnen. Bei Gleichheit dieser beiden gewonnenen Signaturen Su(2) kann auf die Unversehrtheit der Unterschrift bzw. des zugehörigen Datensatzes u(2) geschlossen werden.

In einem zweiten Schritt wird der empfangene Quittungs-Datensatz q mit dem Zertifikat Zq auf Unversehrtheit geprüft. Hierzu wird mit dem Hashverfahren h aus dem Datensatz q die Signatur Sq berechnet. Auf einem zweiten Weg wird diese Signatur Sq über den öffentlichen Schlüssel pk(2) aus dem Zertifikat Zq gebildet. Bei Gleichheit dieser beiden Signaturen Sq kann auf die Unversehrtheit der Quittung bzw. des zugehörigen Datensatzes q geschlossen werden.

Von der Datensicherungseinrichtung DE1 werden dann die Datensätze q, u(2) der Quittung und der Unterschrift an den Fernkopierer Fk1 gegeben. Auf dem Fernkopierer Fk1 kann dann die aus dem Datensatz q reproduzierte Quittung zusammen mit der aus dem Datensatz u(2) reproduzierten Unterschrift ausgedruckt werden. Auch eine schriftliche Darstellung auf einem Bildschirm ist möglich.

Durch das erfindungsgemäße Verfahren ist sichergestellt, daß die empfangsseitig dargestellte, mit einer Unterschrift versehene Quittung mit der Unterschrift des tatsächlichen Empfängers unterzeichnet ist.

Bei einer Variante zu diesem Verfahrensabschnitt wird in der empfangenden Station B eine Signatur Sq' aus dem Quittungs-Datensatz zusammen mit dem Unterschriften-Datensatz q, u(2) gebildet. Aus dieser Signatur Sq' wird mit dem geheimen Schlüssel sk(2) des Empfängers ein Zertifikat Zq' errechnet. In der die Quittung empfangenden Station A wird dann die Prüfung mit diesen Werten durchgeführt.

Wenn der Übertragungsweg für den Dokumenten-Datensatz m von der Station A zur Station B durch ein kryptologisches Verfahren, beispielsweise durch ein asymmetrisches oder ein symmetrisches Verschlüsselungsverfahren, gesichert wird, so ist dieser Übertragungsvorgang einer Zustellung im geschlossenen und versiegelten Kuvert gleichzusetzen. Hierzu wird beispielsweise in der Datensicherungseinrichtung DE1 der sendenden Station A der Dokumenten-Datensatz m verschlüsselt, zur Station B übertragen und dort in der Datensicherungseinrichtung DE2 entschlüsselt. Es können auch die anderen übertragenen Datensätze zwischen den Stationen A und B, beispielsweise der Quittungs-Datensatz q oder die Unterschriften-Datensätze u(1) bzw. u(2) verschlüsselt werden.

Patentansprüche

Hierzu 1 Seite(n) Zeichnungen

1. Elektronisches Einschreibeverfahren bei der digitalen Übertragung eines Dokumentes, bei dem nacheinander folgende Schritte ausgeführt werden:
in einer Sendestation (Station A) wird aus einem zu übertragenden Datensatz (m) des Dokumentes eine Dokumenten-Signatur (Sm) gebildet,
aus der Signatur (Sm) wird durch ein Kryptierverfahren ein Dokumenten-Zertifikat (Zm) gebildet,
ein Datensatz (u(1)) einer persönlichen Unterschrift des Urhebers des Dokumentes ist gesichert mit einem Unterschriften-Zertifikat (Zu(1)) abgespeichert,
der Dokumenten- und der Unterschriften-Datensatz (m, u(1)), die beiden daraus gewonnenen Zertifikate (Zm, Zu(1)) sowie die dazugehörigen Schlüssel (pk(1), pk(Z)) werden zu einer Empfangsstation (Station B) übertragen,
dort wird der Unterschriften-Datensatz (u(1)) mit dem Unterschriften-Zertifikat (Zu(1)) und anschließend der Dokumenten-Datensatz (m) mit dem Dokumenten-Zertifikat (Zm) jeweils durch Berechnung der zugehörigen Signaturen (Su(1), Sm) auf Unversehrtheit überprüft,
die Datensätze (m, u) des Dokumentes und der Unterschrift werden in lesbarer Form ausgegeben,
aus einem zurückzuübertragenden Datensatz (q) einer Quittung wird eine Quittungs-Signatur (Sq) gebildet,
aus dieser Signatur (Sq) wird durch ein Kryptierverfahren ein Quittungs-Zertifikat (Zq) gebildet,
ein weiterer Datensatz (u(2)) einer persönlichen Unterschrift des Empfängers ist gesichert mit einem weiteren Unterschriften-Zertifikat (Zu (2) abgespeichert,
der Quittungs- und der weitere Unterschriften-Datensatz (q, u(2)), die beiden daraus gewonnenen Zertifikate (Zq, Zu(2)) sowie die dazugehörigen Schlüssel (pk(2), pk(Z)) werden zur Sendestation (Station A) zurückübertragen,
dort wird der weitere Unterschriften-Datensatz (u(2)) mit dem weiteren Unterschriften-Zertifikat (Zu(2)) und anschließend der Quittungs-Datensatz (q) mit dem Quittungs-Zertifikat (Zg) jeweils durch Berechnung der zugehörigen Signaturen (Su(2), Sq) auf Unversehrtheit überprüft, und
die Datensätze (q, u(2)) der Quittung und der weiteren Unterschrift werden in lesbarer Form ausgegeben.

2. Elektronisches Einschreibeverfahren nach Anspruch 1, bei dem die Dokumenten-Signatur (Sm') aus dem Dokumenten- zusammen mit dem Unterschriften-Datensatz (m, u(1)) und die Quittungs-Signatur (Sq') aus dem Quittungs- zusammen mit dem weiteren Unterschriften-Datensatz (q, u(2)) gebildet werden.

3. Elektronisches Einschreibeverfahren nach Anspruch 1 oder 2 bei dem die Unterschrift als Unterschriften-Datensatz (u(1), u(2)) in einer Chipkarte (Ck1, CK2) gesichert mit einem Zertifikat (Zu(1), Zu(2)) zusammen mit dem dazugehörigen Schlüssel (pk(Z)) gespeichert ist.

4. Elektronisches Einschreibeverfahren nach einem der Ansprüche 1 bis 3 bei dem zumindest der Dokumenten-Datensatz (m) verschlüsselt übertragen wird.

– Leerseite –

Nummer: DE 44 13 678 C1
Int. Cl.[6]: H 04 N 1/44
Veröffentlichungstag: 4. Mai 1995